We claim:

1. A method of protecting a configuration data sequence against reverse engineering, wherein the configuration data sequence includes a plurality of configuration bits, and is used to configure the operation of a programmable device, the method comprising the steps of:

partially encrypting the configuration bits of the configuration data sequence by altering some, but not all, of the configuration bits;

storing the partially-encrypted configuration data sequence in a memory external to the programmable device;

storing decryption information for the partially-encrypted configuration data sequence in the programmable device;

loading the partially-encrypted configuration data sequence into the programmable device;

decrypting the partially-encrypted configuration data sequence using the decryption information stored in the programmable device; and

configuring internal logic of the programmable device using the decrypted configuration data sequence.

2. The method of claim 1, wherein the partially-encrypted configuration data sequence is loaded into the programmable device via a wireless connection.

3. The method of claim 1, wherein the decryption information includes a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit in the

sequence of bits of the decryption information provides an indication of which bits in the configuration data sequence are encrypted.

4. The method of claim 3, wherein the decrypting step further comprises the step of:

toggling logic values of the bits in the partially-encrypted configuration data sequence that are indicated as being encrypted in the sequence of bits of the decryption information.

5. The method of claim 3, wherein the decrypting step further comprises the step of:

modifying logic values of the bits in the partially encrypted data sequence that are indicated as being encrypted in the sequence of bits of the decryption information using a set of logic values stored in the programmable device.

6. The method of claim 4, wherein the toggling step further comprises the step of:

executing an exclusive-or function between the partially-encrypted configuration data sequence and the sequence of bits of the decryption information.

7. The method of claim 1, wherien the storing decryption information step further comprises the steps of:

storing a first secret sequence in the programmable device, wherein the first secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit of the first secret sequence provides an indication of which bits in the configuration data sequence are encrypted; and

storing a second secret sequence in the programmable device, wherein the second

secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein the bits of the second secret sequence that correspond to the bits of the configuration data sequence that are encrypted have identical values to the corresponding bits of the configuration data sequence.

8. The method of claim 7, wherein the decrypting step further comprises the step of:

overwritting the bits in the partially-encrypted configuration data sequence using the bits of the second secret sequence that correspond to the bits of the first secret sequence that indicate which bits of the configuration data sequence are encrypted.

9. The method of claim 1, wherein the storing decryption information step further comprises the steps of:

providing a one-time programmable memory device within the programmable device; and

programming selected memory cells of the one-time programmable memory device so as to permanently set the logical values stored in the selected memory cells;

wherein the selected memory cells correspond to the bits of the configuration data sequence that are encrypted and the logic values set in the selected memory cells correspond to the actual logic values of the configuration data sequence.

10. The method of claim 9, wherein the decrypting step further comprises the step of:

loading the partially-encrypted configuration data sequence into the one-time programmable memory device.

11. The method of claim 1, wherein the decryption information comprises a list of bit positions within the configuration data sequence that are encrypted.

12. The method of claim 1, wherein the decryption information comprises a list of ordered pairs, each ordered pair including a first value that indicates a bit position in the partially-encrypted configuration data sequence that is encrypted, and a second value that corresponds to an unencrypted value for the bit position from the configuration data sequence.

13. The method of claim 1, wherein the decryption information comprises a list of ordered tuples, each ordered tuple including a first element that indicates a bit position in the partially-encrypted configuration data sequence that is encrypted, a second element that indicates whether the bit of the partially-encrypted configuration data sequence at the indicated bit position is to be modified or overwritten, and a third element that corresponds to an unencrypted value for the bit position from the configuration data sequence.

14. The method of claim 13, wherein the decrypting step further comprises the steps of:

for each ordered tuple in the list,

determining whether the bit of the partially-encrypted configuration data sequence identified by the first element is to be overwritten or modified by examining the second element of the tuple;

if the bit is to be modified, then toggling the value of the bit at the identified bit position in the partially-encrypted configruation data sequence; and

if the bit is to be overwritten, then overwritting the bit at the identified bit position in the partially-encrypted configuration data sequence using the value in the third element of the tuple.

15. An apparatus for protecting a configuration data sequence from reverse engineering, wherein the configuration data sequence includes a plurality of configuration bits, and is used to configure the operation of a programmable device, comprising:

an encrypted configuration data store external to the programmable device for storing a partially-encrypted configuration data sequence, wherein some, but not all, of the bits in the partially-encrypted configuration data sequence are encrypted;

a decryption memory store within the programmable device for storing decryption information;

an interface for loading the partially-encrypted configuration data sequence from the encrypted configuration data store into the programmable device; and

a decryption unit for decrypting the partially-encrypted configuration data sequence uisng the decryption information stored in the decryption memory.

16. The apparatus of claim 15, wherein the interface is a wireless interface.

17. The apparatus of claim 15, wherein the decryption information includes a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit in the sequence of bits of the decryption information provides an indication of which bits in the configuration data sequence are encrypted.

18. The apparatus of claim 17, wherein the decryption unit decrypts the partially-encrypted configuration data sequence by toggling logic values of the bits in the partiall-encrypted configuration data sequence that are indicated as being encrypted in the sequence of bits of the decryption information.

19. The apparatus of claim 17, wherein the decryption unit decrypts the partially-encrypted configuration data sequence by modifying logic values of the bits in the partially-encrypted data sequence that are indicated as being encrypted in the sequence of bits of the decryption information using a set of logic values stored in the programmable device.

20. The apparatus of claim 19, wherein the set of logic values are stored in the decryption memory store.

21. The apparatus of claim 19, wherein the set of logic values are stored in a memory store that is separate from the decryption memory store.

22. The apparatus of claim 15, wherein the decryption memory store includes a first memory store and a second memory store, wherein the first memory store contains a first secret sequence, wherein the first secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit of the first secret sequence provides an indication of which bits in the configuration data sequence are encrypted, and wherein the second memory store contains a second secret sequence, wherein the second

secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein the bits of the second secret sequence that correspond to the bits of the configuration data sequence that are encrypted have identical values to the corresponding bits of the configuration data sequence.

23. The apparatus of claim 22, wherein the decryption unit decrypts the partially-encrypted configuration data sequence by overwritting the bits in the partially-encrypted configuration data sequence using the bits of the second secret sequence that correspond to the bits of the first secret sequence that indicate which bits of the configuration data sequence are encrypted.

24. The apparatus of claim 15, wherein the decryption memory store includes a one-time programmable memory device in which selected memory cells of the one-time programmable memory device are programmed so as to permanently set the logical values stored in the selected memory cells, wherein the selected memory cells correspond to the bits of the configuration data sequence that are encrypted and the logic values set in the selected memory cells correspond to the actual logic values of the configuration data sequence.

25. The apparatus of claim 24, wherein the decryption unit decrypts the partially-encrypted configuration data sequence by loading the partially-encrypted configuration data sequence into the one-time programmable memory device.

26. The apparatus of claim 15, wherein the decryption information comprises a list of bit positions within the configuration data sequence that are encrypted.

27. The apparatus of claim 15, wherein the decryption information comprises a list of ordered pairs, each ordered pair including a first value that indicates a bit position in the partially-encrypted configuration data sequence that is encrypted, and a second value that corresponds to an unencrypted value for the bit position from the configuration data sequence.

28. The apparatus of claim 15, wherein the decryption information comprises a list of ordered tuples, each ordered tuple including a first element that indicates a bit position in the partially-encrypted configuration data sequence that is encrypted, a second element that indicates whether the bit of the partially-encrypted configuration data sequence at the indicated bit position is to be modified or overwritten, and a third element that corresponds to an unencrypted value for the bit position from the configuration data sequence.

29. The apparatus of claim 28, wherein the decryption unit decrypts the partially-encrypted configuration data sequence by:

for each ordered tuple in the list,

determining whether the bit of the partially-encrypted configuration data sequence identified by the first element is to be overwritten or modified by examining the second element of the tuple;

if the bit is to be modified, then toggling the value of the bit at the identified bit position in the partially-encrypted configruation data sequence; and

if the bit is to be overwritten, then overwritting the bit at the identified bit position in the partially-encrypted configuration data sequence using the value in the

third element of the tuple.

30. The apparatus of claim 15, wherein the programmable device is a SRAM-based field programmable gate array (FPGA).

31. The apparatus of claim 15, wherein the programmable device is a reconfigurable logic device.

32. The apparatus of claim 30, wherein the interface includes a plurality of input/output peripheral cells for interfacing between internal elements of the FPGA and a plurality of external circuits.

33. The apparatus of claim 30, wherein the FPGA includes:

a plurality of input/output peripheral cells for interfacing between the FPGA and a plurality of external circuits;

user-configurable logic blocks for performing logical functions as defined by a user of the FPGA;

interconnect elements for connecting the user-configurable logic blocks to the plurality of input/output peripheral cells;

wherein the interconnect elements are configured using the configuration data sequence.

34. The apparatus of claim 30, wherein the decryption memory store is an SRAM memory.

35. The apparatus of claim 30, wherein the decryption memory store is a ROM.